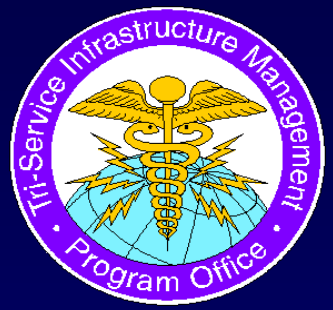


Tri-Service Infrastructure Management Program Office

“How One Worldwide Enterprise Keeps Private Healthcare Information Secure”

HIMSS Conference, 15 February 2005

Presenters

- COL Vaseal M. Lewis
  - Program Manager, Tri-Service Infrastructure Management Program Office (TIMPO)
- Ms Joan Luke
  - Program Manager, Information Assurance, Technology Management Integration and Standards
- Mr Robert Brown
  - TIMPO Technical Services
- Mr Glenn Marshall
  - TIMPO Deployment Services

Overview

- Program Description
- Information Assurance Program Considerations
  - Legislative and Policy
  - Challenges
  - MHS Certification & Accreditation
- Network Protection Program
  - Technical Requirements & Design
- Implementation
  - Schedule
  - Lessons Learned
  - Risk Identification & Mitigation
- Benefits

Learning objectives

1. Identify standards, legislation and policy addressed
2. Define scope of program
3. Present design considerations
4. Review accelerated implementation schedule
5. Summarize successful incorporation of lessons learned and risk identification and mitigation

Program Description

- Purpose
  - Protect privacy, confidentiality, integrity, availability of protected health information (PHI)
- Scope
  - 9.1 million DoD healthcare beneficiaries
  - Over 500 DoD military treatment facilities (MTFs)
    - Army, Navy, and Air Force
  - Department of Veterans Affairs (VA)
  - Regional contractors

Information Assurance Legislative and Policy Drivers

- Public Law 104-199
  Health Insurance Portability and Accountability Act of 1996
- Public Law 107-347 (Title III)
  Federal Information Security Management Act of 2002
- OMB Circular A-130 (Appendix III)
  Security of Federal Automated Information Resources
- DoDI 5200.40
  DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
- DoD 8500 series
  Information Assurance (IA) instructions and directives

Project Challenges

- Clinger-Cohen and OMB A-130 states that "all agencies shall implement and maintain a program to assure that adequate security is provided" for all information collected, processed, transmitted, stored, or disseminated
  - Effectively include IA in Frameworks
  - Integrate IA into system design and development

MHS Certification & Accreditation Process

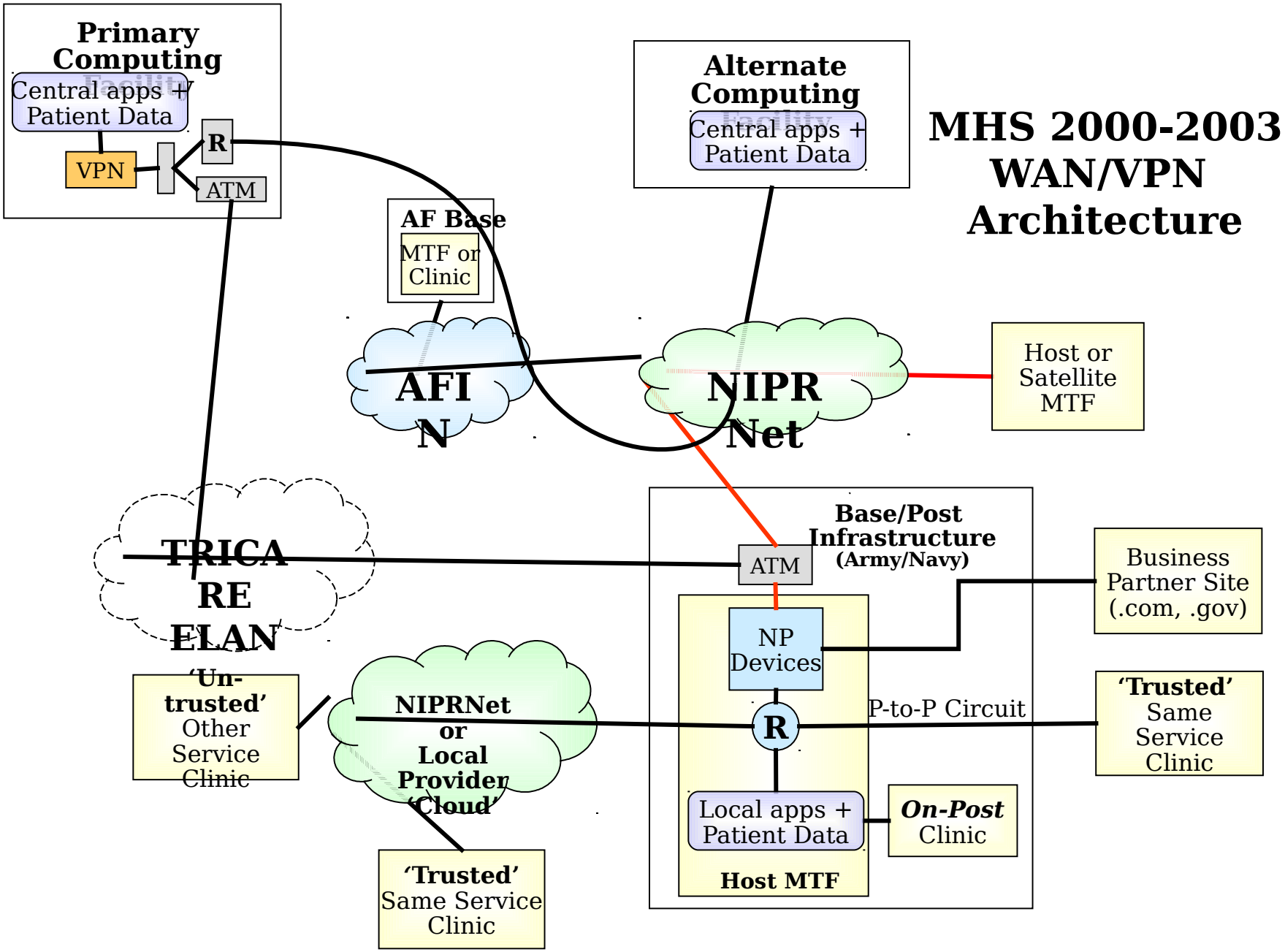
- Identifies policies, standards, and security technologies necessary to protect information assets
- Information Assurance Program achieves compliance of the IA principles through the Certification and Accreditation process
  - Confidentiality
  - Integrity
  - Availability
  - Authentication/ID
  - Non-repudiation

MHS Network Protection Program

- Provides –
  - Standards based infrastructure solution
    - Protecting MHS networks and data exchanges between secure healthcare enclaves
  - Support and processes for design, deployment, and sustainment of standard MHS solution
    - Joint effort executed with Services and key stakeholder organizations

Baseline Environment

- Legacy architecture based primarily on geography and workflow
  - Without regard to Service, site, or security
- Large variations in communication topology
- Direct/indirect communications with business partners


Primary Computing Facility
Central apps + Patient Data
VPN
R
ATM
Alternate Computing Facility
Central apps + Patient Data
MHS 2000-2003 WAN/VPN Architecture
AF Base
MTF or Clinic
AFIN
NIPR Net
Host or Satellite MTF
TRICARE ELAN
Base/Post Infrastructure (Army/Navy)
ATM
Business Partner Site (.com, .gov)
NP Devices
'Un-trusted' Other Service Clinic
NIPRNet or Local Provider 'Cloud'
R
P-to-P Circuit
'Trusted' Same Service Clinic
Local apps + Patient Data
On-Post Clinic
Host MTF
'Trusted' Same Service Clinic

Design Requirements

Solution must –

- Provide underlying standards based infrastructure to protect against loss/unauthorized disclosure of patient information
- Meet Federal/DoD/Service standards for security and encryption
- Meet/exceed the WAN availability requirement
  - Supporting Mission Essential/Mission Critical (ME/MC) applications

Design Requirements
(continued)

Solution must –

- Meet functional requirements for encryption
- Support current and future application data flows
- Provide visibility and manageability
  - Without compromising security of the Service healthcare enclave

Design Requirements
(continued)

Solution must –

- Support administration agreements
  - Multi-level domain management responsibilities
  - Central help desk and engineering support
- Support Service unique requirements
  - Air Force VPN Mesh between AF Base networks and AF Gateway
    - DISA managed MHS-VPN device deployed to Community of Interest (COI) network sites

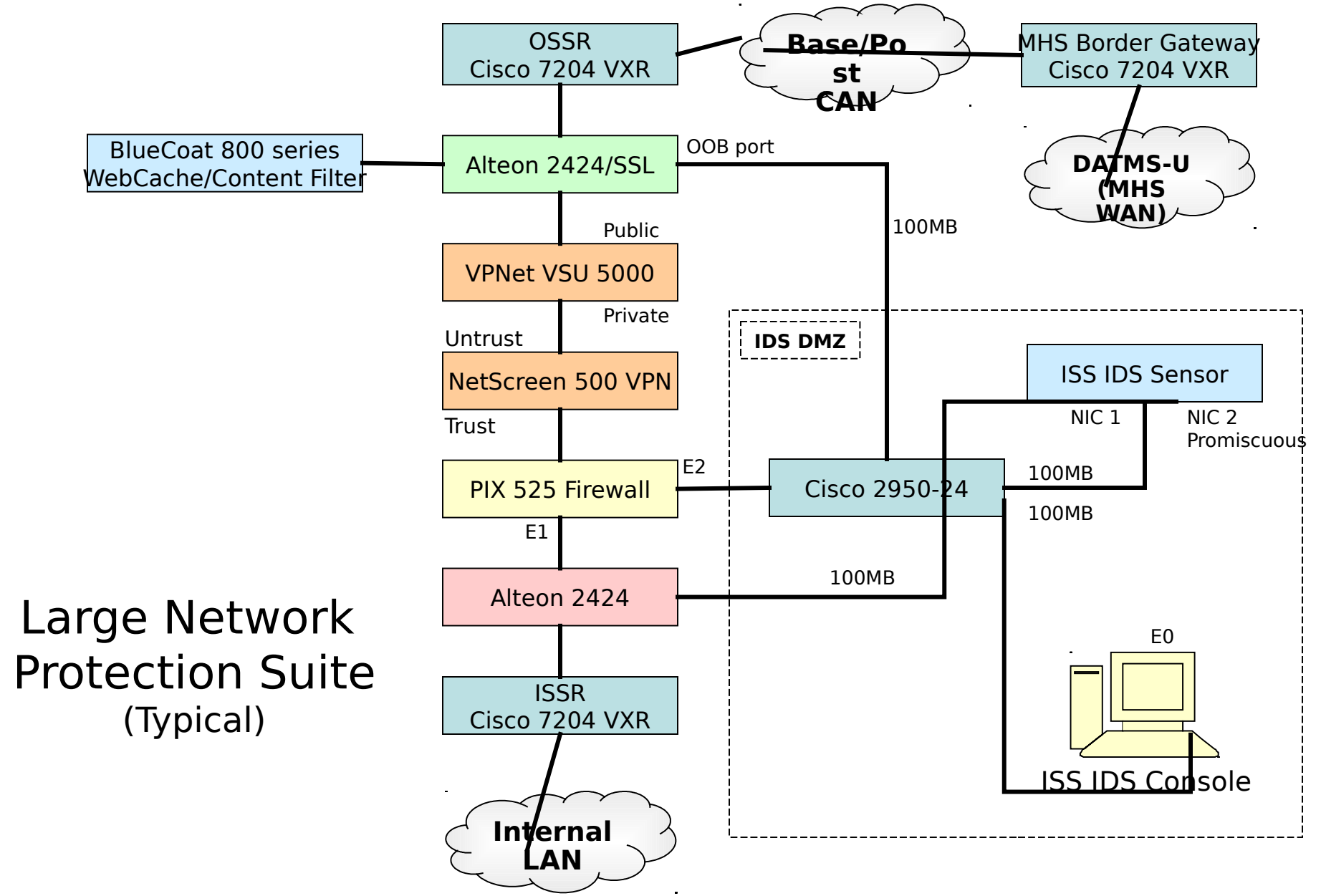
Technical Solution

Three primary components

- TIMPO *Large* Security Suite
  - Provides basic framework for DoD compliant multi-layer protection scheme for MHS healthcare enclaves
- MHS Virtual Private Network (VPN) Domain
  - Protects sensitive information in transport
- Small Security Suites
  - Extends capability to satellite clinics
  - Maintains integrity of local Service/site enclave

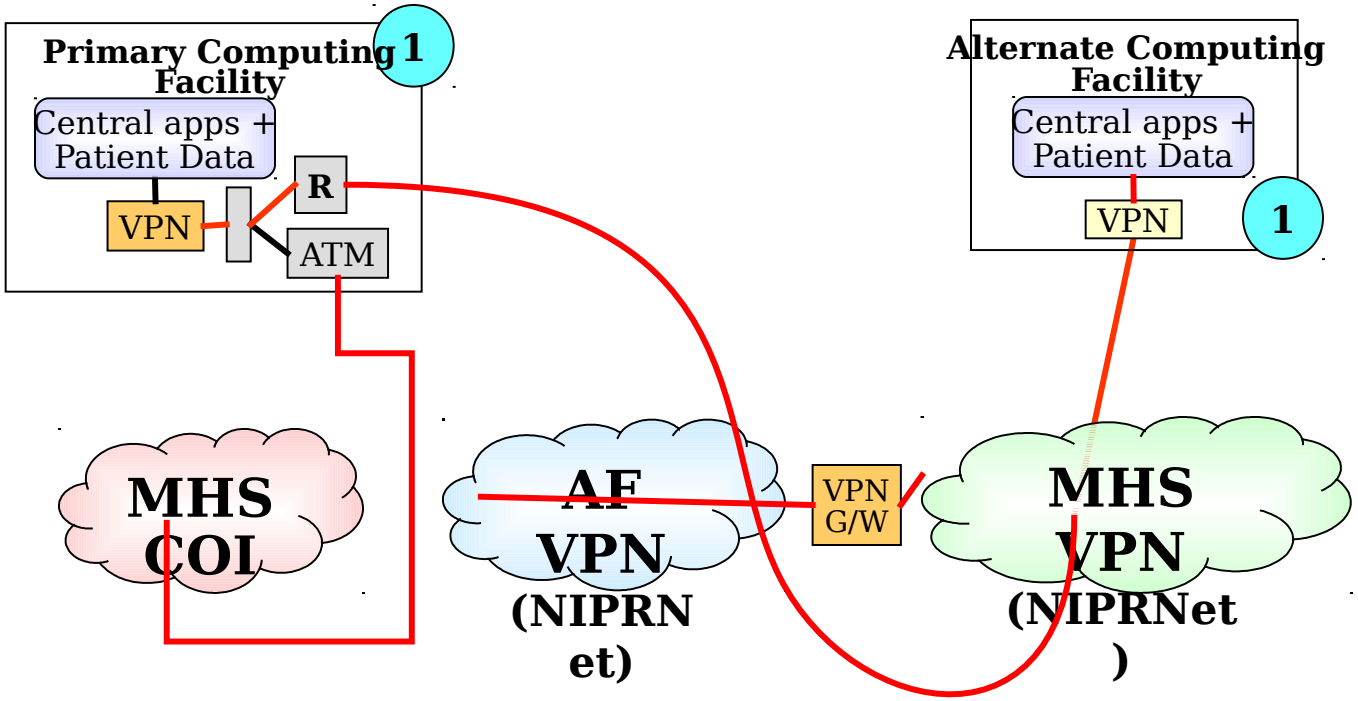
Large Security Suite

- Protocol and application independent architecture
  - Compliant with Industry and Government standards
  - High performance and highly scaleable design
- “Best of Breed”, commercial-off-the-shelf
  - Standard configurations per site size
- Implementation completed in FY03
- VPN/NP Working Group started in March 2003

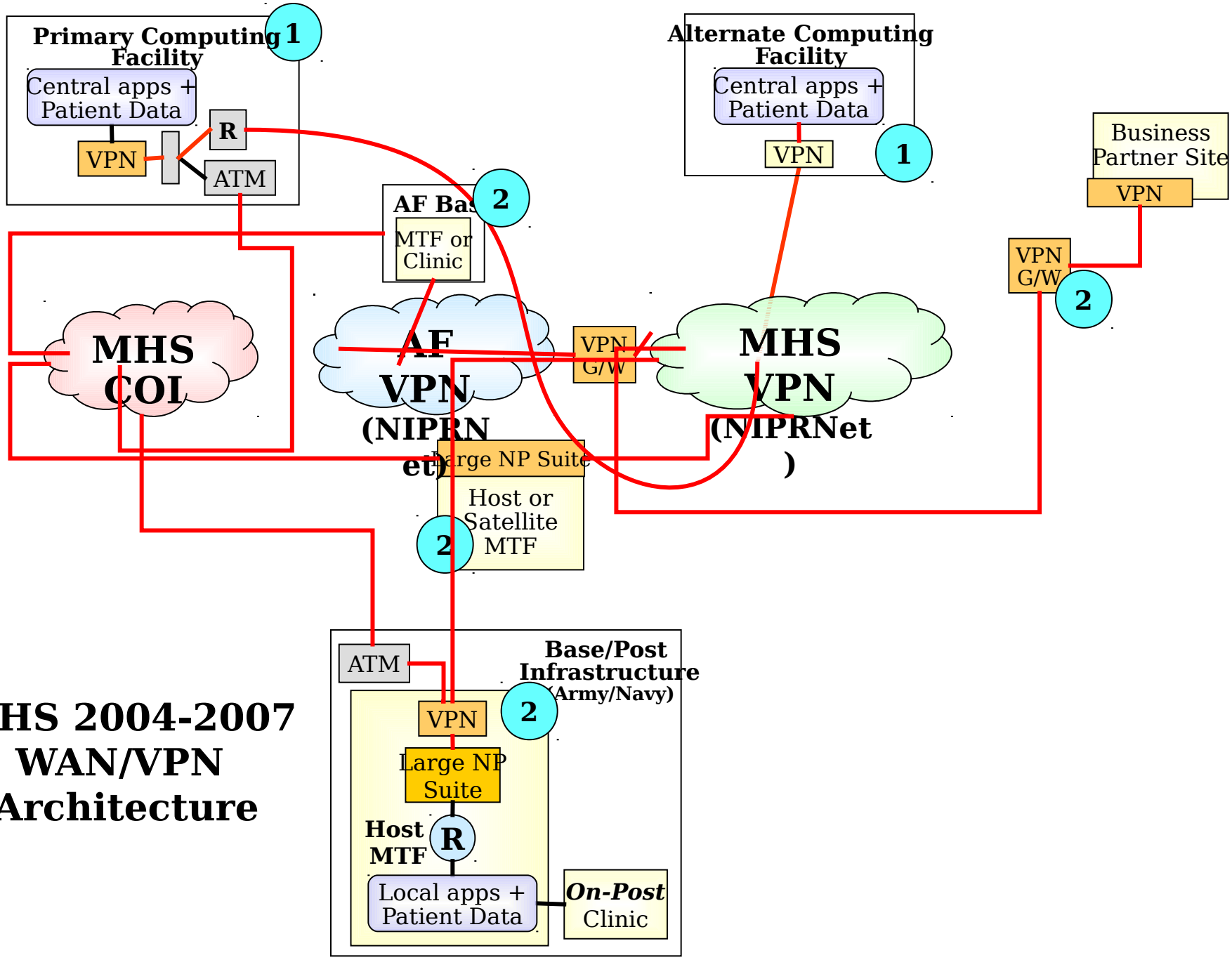

OSSR
Cisco 7204 VXR
Base/Post
CAN
MHS Border Gateway
Cisco 7204 VXR
DATMS-U
(MHS
WAN)
BlueCoat 800 series
WebCache/Content Filter
Alteon 2424/SSL
OOB port
100MB
Public
VPNet VSU 5000
Private
Untrust
NetScreen 500 VPN
Trust
PIX 525 Firewall
E2
E1
Alteon 2424
ISSR
Cisco 7204 VXR
Internal
LAN
IDS DMZ
ISS IDS Sensor
NIC 1
NIC 2
Promiscuous
Cisco 2950-24
100MB
100MB
100MB
E0
ISS IDS Console
Large Network
Protection Suite
(Typical)

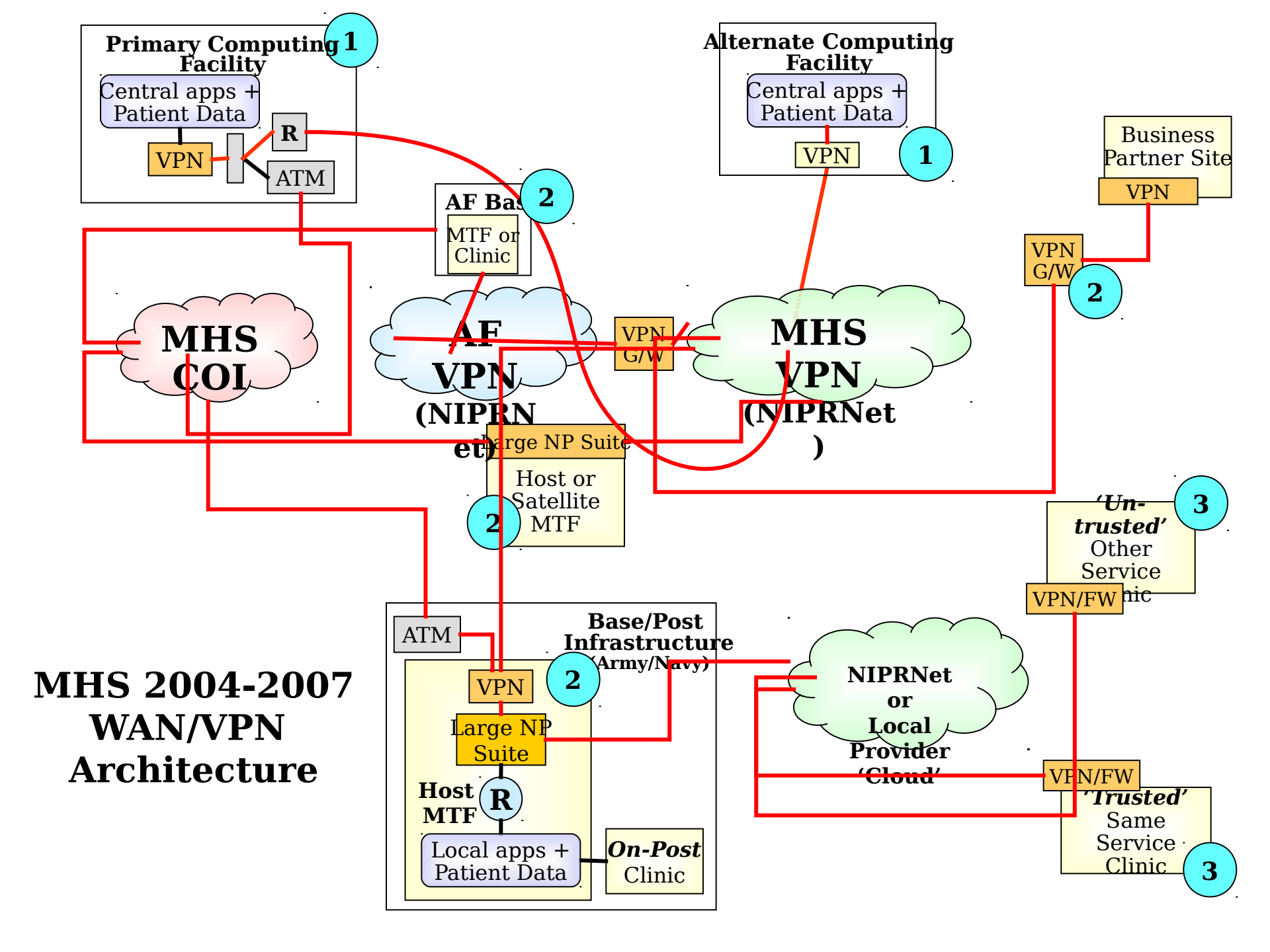
MHS VPN Design

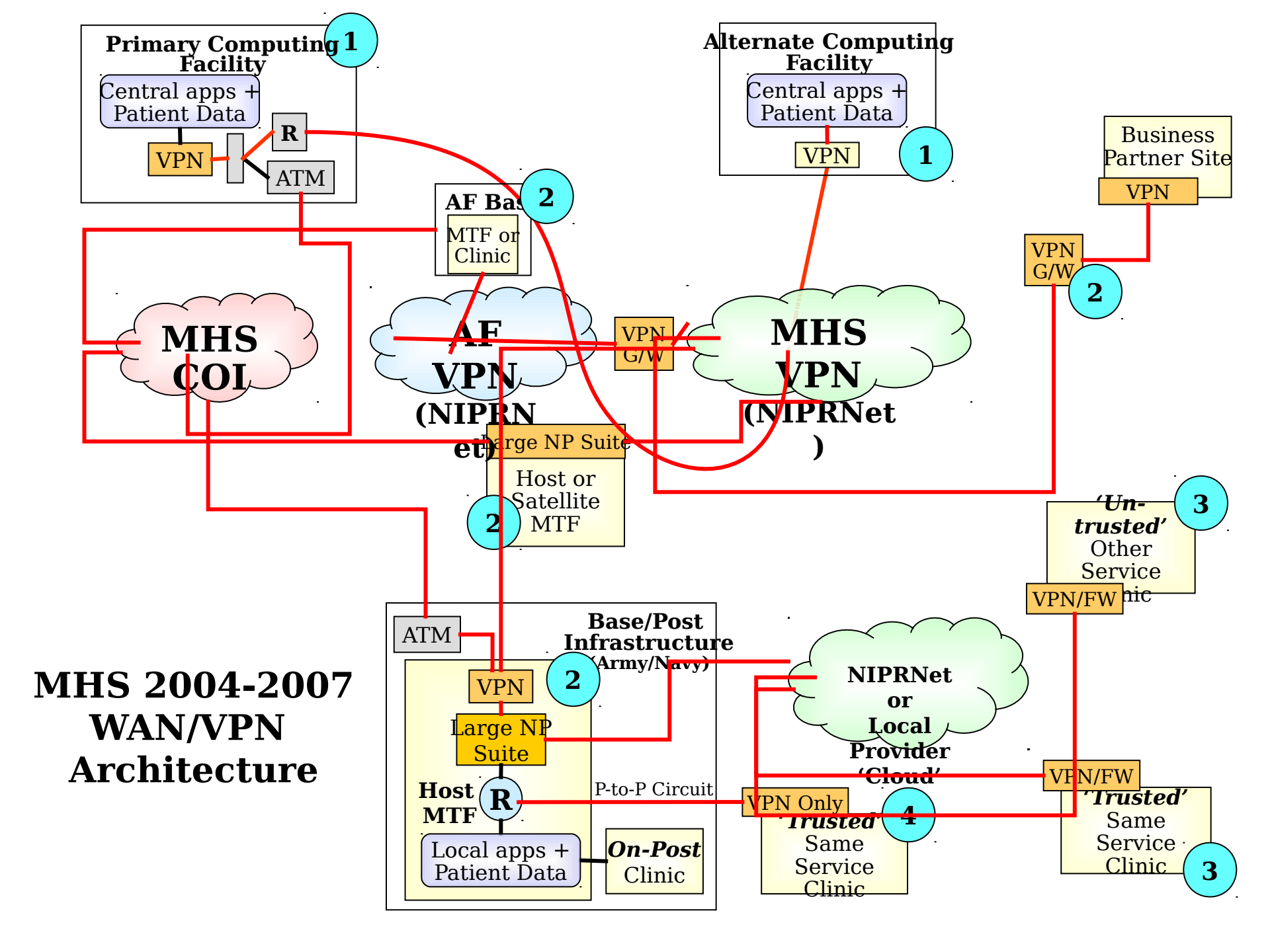
- Architecture model developed by Joint Working Group
- Model included –
  - "Mesh"
    - Protect sensitive information in transport between secure MHS sites
  - Gateway sites
    - Connect other Service or Agency networks to MHS VPN "Mesh"
  - MHS COI network
    - For secure mission essential/mission critical transport
- Model structured in simple four tier structure



MHS 2004-2007 WAN/VPN Architecture


Primary Computing Facility
1
Central apps + Patient Data
VPN
R
ATM
Alternate Computing Facility
Central apps + Patient Data
VPN
1
Business Partner Site
VPN
VPN G/W
2
AF Bas
2
MTF or Clinic
MHS COI
AF VPN (NIPRNet)
VPN G/W
MHS VPN (NIPRNet)
Large NP Suite
Host or Satellite MTF
2
ATM
Base/Post Infrastructure (Army/Navy)
VPN
2
Large NP Suite
Host MTF
R
Local apps + Patient Data
On-Post Clinic
MHS 2004-2007 WAN/VPN Architecture

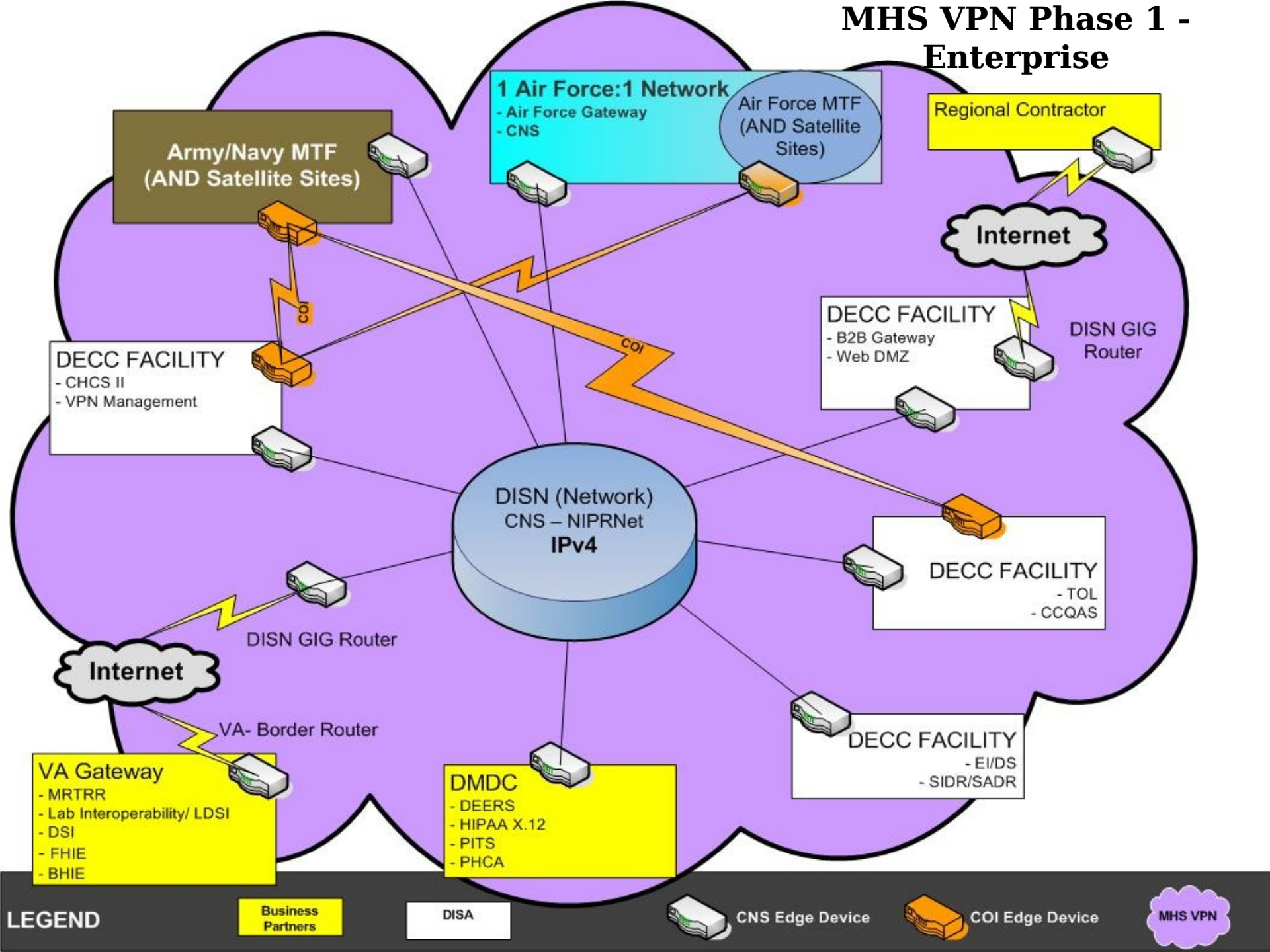

MHS 2004-2007 WAN/VPN Architecture
Primary Computing Facility
1
Central apps + Patient Data
VPN
R
ATM
Alternate Computing Facility
Central apps + Patient Data
VPN
1
Business Partner Site
VPN
VPN G/W
2
AF Bas
2
MTF or Clinic
MHS COI
AF VPN (NIPRNet)
VPN G/W
MHS VPN (NIPRNet)
Large NP Suite
Host or Satellite MTF
2
'Un-trusted' Other Service
3
VPN/FW
ATM
Base/Post Infrastructure (Army/Navy)
VPN
2
Large NP Suite
Host MTF
R
Local apps + Patient Data
On-Post Clinic
NIPRNet or Local Provider 'Cloud'
VPN/FW
'Trusted' Same Service Clinic
3


MHS 2004-2007 WAN/VPN Architecture
Primary Computing Facility
1
Central apps + Patient Data
VPN
R
ATM
Alternate Computing Facility
Central apps + Patient Data
VPN
1
Business Partner Site
VPN
VPN G/W
2
AF Bas
2
MTF or Clinic
MHS COI
AF VPN (NIPRNet)
VPN G/W
MHS VPN (NIPRNet)
Large NP Suite
Host or Satellite MTF
2
'Un-trusted' Other Service
3
VPN/FW
ATM
Base/Post Infrastructure (Army/Navy)
VPN
2
Large NP Suite
Host MTF
R
P-to-P Circuit
Local apps + Patient Data
On-Post Clinic
NIPRNet or Local Provider 'Cloud'
VPN/FW
VPN Only
'Trusted' Same Service Clinic
4
'Trusted' Same Service Clinic
3

MHS VPN Phase 1 Implementation

- Driven by leadership, stakeholders and law
  - Supported by work group through rapid deployment
- Used VPN hardware deployed with Large Suites
- Enterprise data centers (Tier 1 sites) as “Hub” Sites
  - With VPNs to Tier 2 sites
- VPN ‘Mesh’ created with addition of Tier 2 sites
- Designed and deployed VPN Gateways
  - To critical business partners (.com, .mil, .gov)

MHS VPN Phase 1 - Enterprise

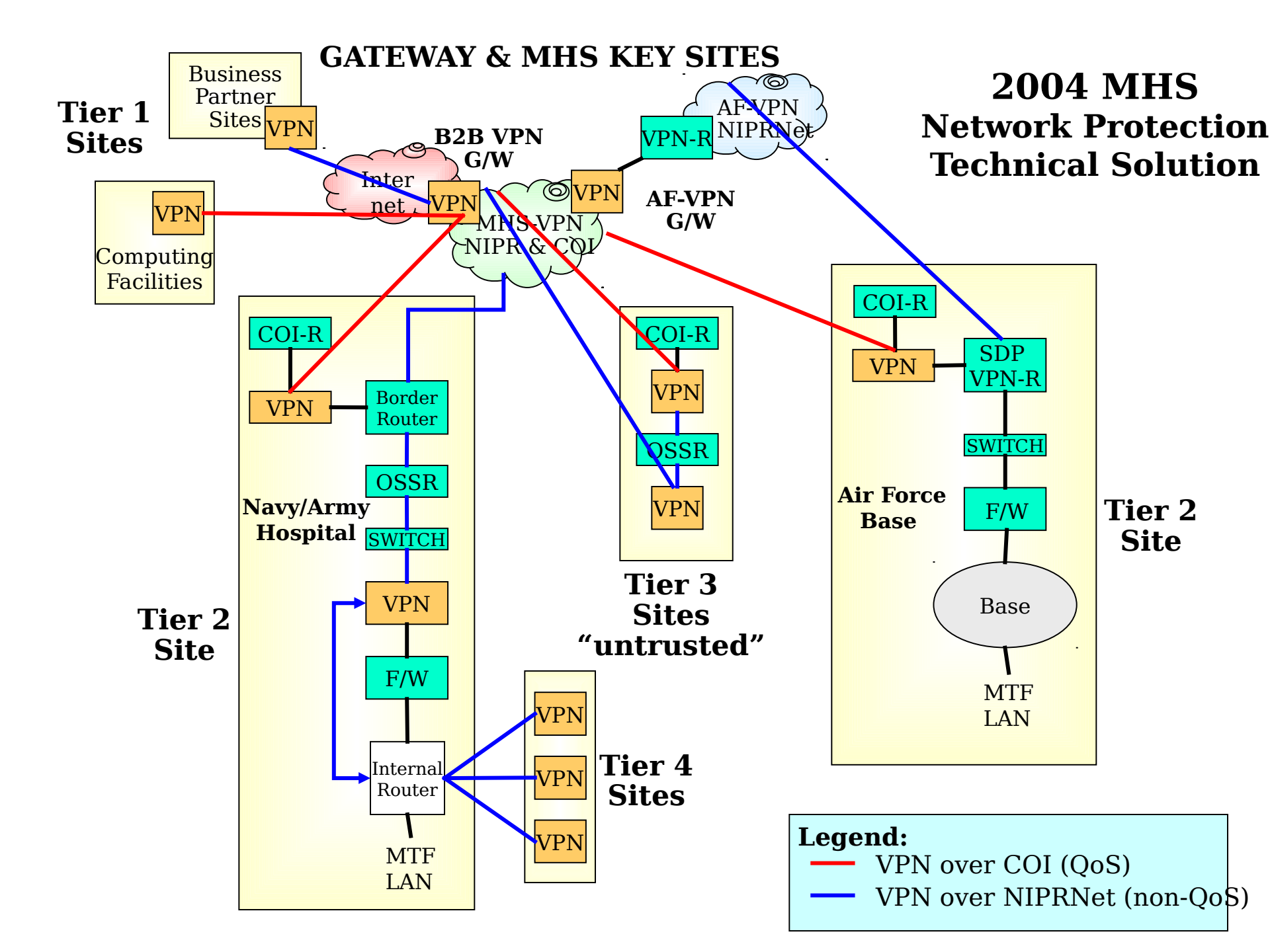


MHS VPN Phase 2 Implementation

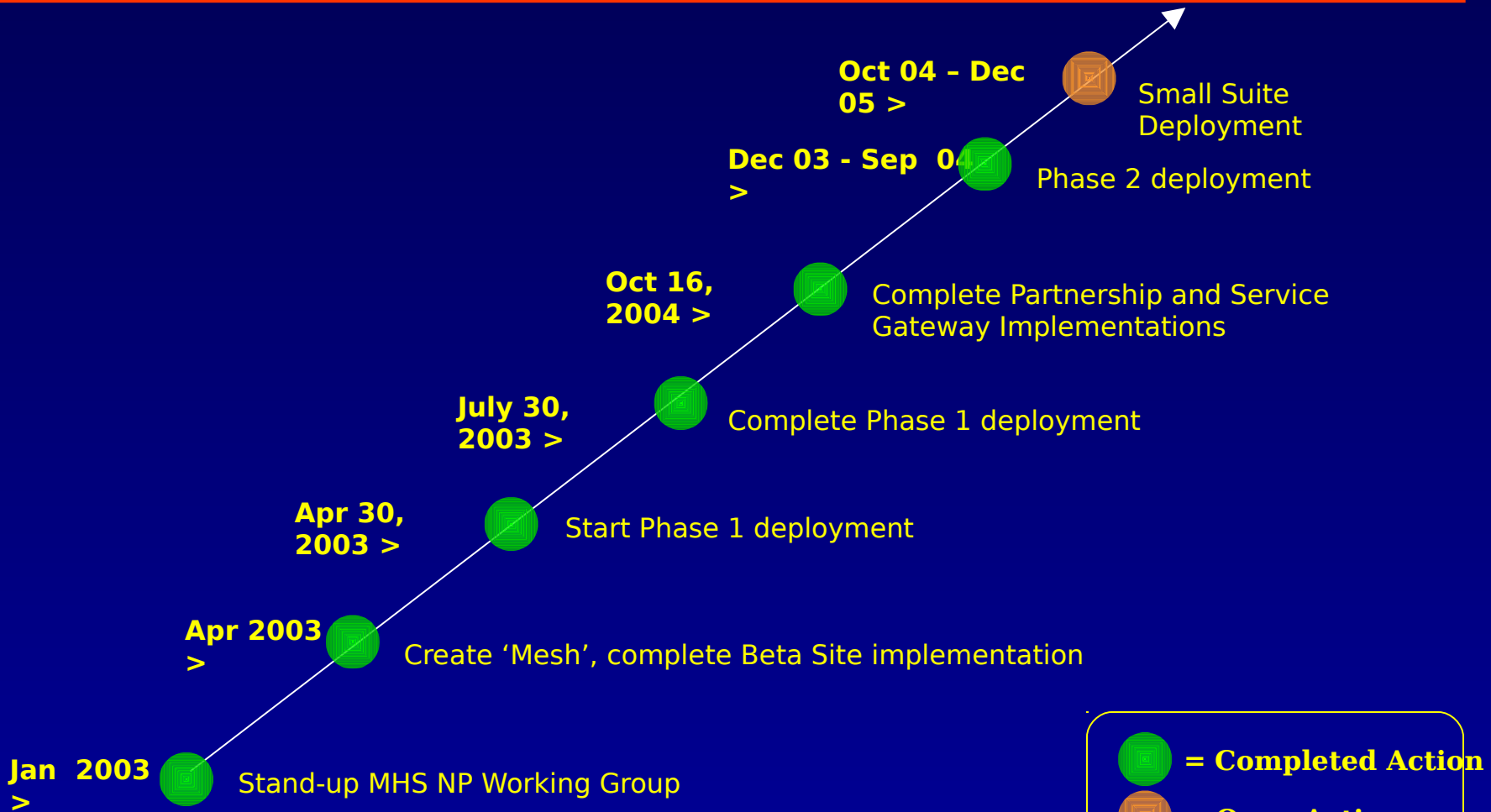
- New VPN domain using route based solution
  - Eliminates maintenance and reliability issues
- Incorporated with previously scheduled technology refresh cycle for original Large Suites
- New devices operated in parallel to legacy VPN
  - Minimize risk of interruption in service at sites

Small Suites Program

- Four tier NP architecture model provides basis for assessing relative risk and projecting NP requirements for Satellites
- Extends Host/Parent MTF enclave protections to off base/post clinics
  - Secures all communications to remote sites
- Leverages virtual systems capability of NetScreen VPN
- Separate tunnels defined for mission essential/mission critical and common network services applications transport


GATEWAY & MHS KEY SITES
2004 MHS
Network Protection
Technical Solution
Tier 1
Sites
Business
Partner
Sites
VPN
B2B VPN
G/W
Inter
net
VPN
MHS-VPN
NIPR & COI
VPN
AF-VPN
G/W
VPN-R
AF-VPN
NIPRNet
VPN
Computing
Facilities
COI-R
VPN
Border
Router
OSSR
Navy/Army
Hospital
SWITCH
VPN
F/W
Internal
Router
MTF
LAN
Tier 2
Site
COI-R
VPN
OSSR
VPN
Tier 3
Sites
"untrusted"
VPN
VPN
VPN
Tier 4
Sites
COI-R
VPN
SDP
VPN-R
SWITCH
Air Force
Base
F/W
Base
MTF
LAN
Tier 2
Site
Legend:
VPN over COI (QoS)
VPN over NIPRNet (non-QoS)

Implementation Schedule



Critical Success Factors

- Governance
  - Program oversight at executive management level
    - From the MHS Chief Information Officer
  - Joint MHS Network Protection (NP) Working Group
    - Ensured rapid response to address
      - Program requirements
      - Critical outages
      - Process improvement

Critical Success Factors
(continued)

- Configuration Management Process
  - Change control process as part of existing processes
    - MHS Infrastructure Configuration Coordination Board (MI-CCB)
  - Formal configuration management reports
    - Document results / problems in near real time
  - Special cases through Joint MHS NP Working Group

Critical Success Factors
(continued)

- Standard Architecture
  - Prior to FY 03, architecture variations led to –
    - Inconsistent applications of security policies
    - Variations in services available to individual sites
    - Difficulty troubleshooting and planning new implementations
  - Standard architecture maintains “defense in depth” services
  - Management responsibilities defined for each layer
    - Consistent application of enterprise policies while enabling local control

Lessons Learned

- Complete rigorous analysis of the requirements and proposed solution
- Establish monitoring, reporting, and management processes prior to deployment and activation
- Define processes and communicate/involve all key stakeholders
- Ensure ongoing coordination of subsequent network changes

Lessons Learned
(continued)

- Create and use a test environment
  - Prove and validate procedures before full scale development
- Analyze and assess risks for every change
  - Include risk mitigation at every site implementation
- Break the implementation into manageable pieces
  - Set priorities

Risk Identification and Mitigation

Risk	Mitigation
• Solution would not be operational by Oct 16, 2003 deadline for compliance with HIPAA transaction standards	• Implementation priorities and support by senior leadership • Involvement of key stakeholders throughout the process using work group
• Resistance to enterprise solution, in environment of decentrally managed solutions	• Involvement of key stakeholders throughout the planning and implementation using work group • Open process and communication regarding implementation and operations

Risk Identification and Mitigation
(continued)

Risk	Mitigation
• Implementation problems due to incorrect sequencing or parallel implementation of changes	• Implementation of disciplined, defined VPN change management process • Incorporated in existing configuration control board processes
• Increased unplanned network downtime due to VPN maintenance	• Established specific VPN maintenance windows
• MHS-VPN “Mesh” changes impact devices or sites other than those intended	• Logical grouping of objects within the “Mesh” • Shift to route based design in final solution

Benefits

- Provides standard enterprise-wide, application independent solution to protect healthcare data traffic
  - Increases protection of patient information
  - Reduces risk of patient harm from disclosure of sensitive information
- Enables compliance with legislative and policy requirements
- Secures data sharing between MHS and business partners
- Maximizes the MHS IM/IT investment
  - Increases access and use of IT solutions and individual and population level healthcare data

Additional Questions

- TIMPO Webpage
  - http://www.tricare.osd.mil/peo/timpo/default.htmadd
- Phone
  - 703-681-6123
- Booth #6354